UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/721,504	11/26/2003	Franck Le	800.0186.U1(US)	6168

29683 7590 12/07/2009

HARRINGTON & SMITH, PC
4 RESEARCH DRIVE, Suite 202
SHELTON, CT 06484-6212

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
12/07/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/721,504	LE ET AL.	
	Examiner	Art Unit	
	MATTHEW T. HENNING	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _22 September 2009_.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1,2,4,11-15,18,42,43,50-56,59,60,62-64 and 66-68_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1,2,4,11-15,18,42,43,50-56,59,60,62-64 and 66-68_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _11/26/2003_ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 9/22/2009.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 9/22/2009 have been fully considered but they are not persuasive.

The arguments pertaining to the amendments made to the independent claims are moot in view of the new grounds of rejection presented below.

The following has been repeated from previous office actions as the applicants have maintained the arguments from previous communications.

Regarding the applicants' argument that the header of the packet of Gupta does not contain "all" of the generated validity information necessary to perform the validity check, the examiner still does not find this argument persuasive. The applicants' use the language "all necessary information required for performing a validity check" throughout the specification. In order to remain consistent with the specification, the examiner has looked to the instant specification in order to interpret the usage of this language, for the purposes of searching and applying prior art. The specification provides evidence that this limitation means "all necessary information required for performing a validity check **without the checking entity needing to further communicate with the sending network node**", as the specification clearly shows that the checking node does not require further communication with the sending node in order to perform the validity checking, but that the checking entity may need to receive additional information from somewhere (i.e. a certificate authority) in order to perform the validity checking. As such, if Gupta disclosed that the key was retrieved from the DNS server, or that

the algorithm to perform the verification was known by the verifier, this would still fall within the scope of the language, in light of the specification. Therefore, the examiner does not find the argument persuasive.

Regarding the applicants' argument that Gupta does not disclose that "no pre-established security association is needed to verify the packet" because the sender has the key before the verification is performed, the examiner does not find the argument persuasive. The instant specification paragraph 0054 further states, with regards to the lack of pre-established security association, that "the nodes do not need to have any pre-established [security association], or have to exchange key values beforehand". The fact that the keys were generated before the fingerprint is encrypted at the sender does not mean there was a pre-established security association between the communicating nodes. In fact, Fig. 7 of Gupta shows that the recipient node does not necessarily have the key before the communication. Furthermore, the instant specification paragraph 0004 indicates that a security association is part of IPSec, but Gupta does not disclose the use of IPSec, and that the security association is "a set of policy and key(s) used to protect information". Gupta does not disclose such security association existing before the communication. As such, the examiner does not find the argument persuasive.

Regarding the applicants' argument, with respect to previous claim 5 which is now incorporated into the independent claims, that Gupta did not disclose wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the examiner does not find the argument persuasive. The applicants appear to believe that the claim language requires that the algorithm itself or an indication of what algorithm should be used be included in the validity information. However, this is not the case.

Rather, the claim language requires that values to initialize an algorithm be included in the validity information. To initialize is to assign an initial value. In other words, the claim requires that an initial value be input to the algorithm. Col. 7 Paragraph 2 clearly shows that the encrypted signature is decrypted. In order for this to occur, the encrypted signature must "initialize" the decryption algorithm. As such, the examiner does not find the argument persuasive.

Further, rather than claiming what the invention is not, the examiner suggests that the applicants carefully consider the meets and bounds of their invention, and then carefully construct positive claim limitations which accurately define that scope. For example, if the applicants believe that it is important to their invention that the algorithm and key used for verification is provided in the header of the packet, then the applicants should particularly point that out in the claim language.

All objections and rejections not set forth below have been withdrawn.

Claims *1,2,4,11-15,18,42,43,50-56,59,60,62-64 and 66-68* have been examined.

Claim Objections

Claim 62 is objected to because it has not been listed in the claim listing. However, in order to not increase the pendency of this application, the examiner will use the previous version of claim 62 in examining the claims. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 66-68 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed towards “a computer program configured to operate on a computer readable storage medium, that when executed controls a processor to perform:”. As such, the claims are actually only directed towards the computer program *per se* and not the medium. A computer program *per se* does not fall within one of the four statutory categories of invention, and therefore the claims are rejected for failing to meet the requirements of 35 USC 101.

Claim Rejections - 35 USC § 103

Claims 1-2, 15, 18, 42-43, 54-56, 59-60, and 62-64, and 66-68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (US Patent Number 6,389,532) hereinafter referred to as Gupta, and further in view of Mitreuter et al. (US Patent Application Publication 20030033375) hereinafter referred to as Mitreuter.

Regarding claims 1 and 66, Gupta disclosed a method (See Gupta Fig. 1 Element 104, 108 or 112), comprising the steps of: generating validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4), wherein the validity information comprises all necessary information required to perform a validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2); the validity information comprising algorithm information to be used for performing the validity check of the packet and no pre-established security association is needed to verify the packet and algorithm initialization information(See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); generating a packet header (302), comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4) ; and sending the packet including the packet header from a first network node to a second network node (See Gupta Col. 6 Paragraph

4), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet.

Regarding claim 18, Gupta disclosed an apparatus comprising: validity information generating means for generating validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4); packet header generating means for generating a header for the packet, comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); and sending means for sending the packet including the header to a receiving network node (See Gupta Col. 6 Paragraph 4), wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2) and the validity information comprises algorithm information to be used for performing the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6

Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet.

Regarding claim 42, Gupta disclosed an apparatus, comprising: a validity information generator configured to generate validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4); a packet header generator configured to generate a header for the packet, comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); and a transmitter configured to send the packet including the header to a receiving network node (See Gupta Col. 6 Paragraph 4), wherein the validity information comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 3 - Col. 7 Paragraph 2), wherein the algorithm information comprises values to initialize an algorithm to be

used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet.

Regarding claim 55, Gupta disclosed an apparatus, comprising: a receiver configured to receive packets from a sending network node (See Gupta Fig. 1 Element 108, Fig. 7 and Col. 6 Paragraph 5); and a checker configured to perform a validity check of a packet by referring to validity information contained in a header of the packet and no pre-established security association is needed to verify the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required to perform the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2), and the validity information comprises algorithm information to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4), wherein the algorithm information comprises values

to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet.

Regarding claim 59, Gupta disclosed an apparatus, comprising: a transmitter configured to forward packets from a sending network node to a receiving network node (See Gupta Fig. 7 and Col. 6 Paragraph 5); and a checker configured to perform a validity check of a packet by referring to validity information contained in a header of the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2), and the validity information comprises algorithm information to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4), wherein the algorithm information comprises values

to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet.

Regarding claims 63 and 67, Gupta disclosed a method comprising: receiving packets (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2); and performing a validity check of a packet by referring to validity information contained in a header of the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required for performing the validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 3 - Col. 7 Paragraph 2), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6

Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet.

Regarding claims 64 and 68, Gupta disclosed a method comprising: forwarding received packets (Gupta Col. 7 Paragraph 2); and performing means for performing a validity check of a packet by referring to validity information contained in a header of the packet (Gupta Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 3 - Col. 7 Paragraph 2), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach

the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter in the packet verification system of Gupta by included the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet.

Regarding claims 2, 43, 56 and 60, Gupta and Mitreuter disclosed that the generating of the validity information comprises generating security information indicating security services applied to the packet (See Gupta Col. 5 Paragraph 7).

Regarding claim 62, Gupta and Mitreuter disclosed that the generating of the validity information comprises generating public key information of a sending node (See Mitreuter Paragraph 0037).

Regarding claim 15 and 54, Gupta and Mitreuter disclosed signing the packet using a private key corresponding to the public key indicated by the validity information in the packet header in a sending network node (See Gupta Col. 6 Paragraph 4 and Mitreuter Paragraph 0037).

Claims 4, 12-14, and 51-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta and Mitreuter as applied to claims 1 and 42 above, and further in view of Naudus (US Patent Number 6,202,081).

Regarding claims 12-14, and 51-53, Gupta and Mitreuter disclosed validation of packets, but failed to disclose that the step of generating the validity information comprises generating an information item for preventing replay attacks.

Naudus teaches that in a packet filtering system, packets should include timestamps in order to prevent replay attacks. Naudus further teaches that "[r]eplay attacks occur when a malicious user gains access to a router or other network device on a computer network that is forwarding data packets. Legitimate data packets are intercepted and then re-sent at a later time to allow the malicious user to appear as a legitimate user. A firewall helps prevent replay attacks by checking a time-stamp in the data packet that prevents the data packets from being re-sent at a later time." (See Naudus Col. 2 Paragraph 4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Naudus in the packet validity checking system of Gupta and Mitreuter by including a timestamp in each packet and verifying the timestamp at the validity checker. This would have been obvious because the ordinary person skilled in the art would have been motivated to prevent replay attacks in the network. In this combination, the inclusion of a timestamp in each packet, in itself, is an indication of a procedure to be used for anti replay attacks.

Regarding claim 4, Gupta and Mitreuter did not specifically teach that the step of generating the algorithm information comprises generating the algorithm information which

indicates an algorithm to be used for performing the validity check of the packet. However, as taught by Naudus, in Col. 6 Line 60 - Col. 7 Line 7, it is well known to include in the packet header, an identification of which algorithm was used to sign the packet. As such, it would have been obvious to have included this information within the packet. Furthermore, the ordinary person skilled in the art at the time of invention would have recognized that this would allow for the user of a multiplicity of signature algorithms, as well as allowing updating of the signature algorithms in the future, and therefore it would have been obvious to have included an indication of the signature algorithm in the packet.

Claims 11, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta and Mitreuter as applied to claims 6 and 23 above, and further in view of Nikander (US Patent Number 7,155,500).

Gupta and Mitreuter disclosed including public key information within the packets, including the public key itself within the packets, but failed to specifically disclose that the step of generating the public key information comprises generating public key verification information indicating information in order to verify that the public key actually belongs to the sending node. Gupta did disclose that the public and private key pairs can be generated and stored in a certification server (See Col. 4 Paragraph 2).

Nikander teaches that by including the certificate of the public key, the receiving host can verify that the public key is truly owned by the sender (See Nikander Col. 10 Line 50 – Col. 12 Line 9).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Nikander in the packet verification system of Gupta and

Mitreuter by including the public key certificate within each packet and verifying that the sender of each packet owned the public key used to sign the packet. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that a malicious node was not claiming to be a different node.

Conclusion

Claims 1,2,4,11-15,18,42,43,50-56,59,60,62-64 and 66-68 have been rejected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571)272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Primary Examiner, Art Unit 2431